RSA NETWITNESS® PLATFORM

NetWitness UEBA Quick Start Guide

for RSA NetWitness® Platform 11.4

Contact Information

RSA Link at https://community.rsa.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

June 2020

What is NetWitness UEBA?

RSA NetWitness UEBA (User and Entity Behavior Analytics) is an advanced analytics solution that empowers enterprise SOC managers and analysts to discover, investigate, and monitor risky behaviors across entities namely Users and Network in your environment. NetWitness UEBA enables analyst to:

- Detect
  - malicious and rogue users
  - abnormal network traffic
- Pinpoint high-risk behaviors
- Discover attacks
- Investigate emerging security threats
- Identify potential attacker's activity

About this Guide

This guide provides end-to-end instructions to configure NetWitness Platform UEBA and to use UEBA features.

RSA NetWitness Platform 11.4 Documentation in RSA Link

NetWitness Platform product documentation is organized along functional lines. If you are looking for a specific guide or version, go to the Version 11.x Master Table of Contents.

Use these links to view the RSA NetWitness Platform 11.4 documentation. Both links provide the same documentation, in these two formats:

- HTML Guides include the latest information for currently supported 11.x versions: RSA NetWitness Platform 11.x Documentation.
- PDF Guides provide the information for a specific version: RSA NetWitness Platform 11.4 PDFs.

Use these links to access documentation that is not related to a particular version of the software:

- Hardware setup guides: https://community.rsa.com/community/products/netwitness/hardware-setup-guides.
- Documentation for RSA Content such as feeds, parsers, application rules, and reports: https://community.rsa.com/community/products/netwitness/rsa-content.

Getting Started

The following tasks can be performed in any sequence.

Description	References
	
View information about product updates, improvements, and known issues.	Release Notes
Understand NetWitness UEBA	*RSA NetWitness UEBA User Guide*

Setup and Installation

Standalone Installation

The following tasks must be performed in the following sequence.

Description	References
	
Review the supported hardware.	"System Requirement" topic in *UEBA Standalone Installation Guide*
Review the UEBA deployment.	"RSA NetWitness UEBA Standalone Installation " topic in *UEBA Standalone Installation Guide*
Configure the ports on your firewall.	"RSA NetWitness UEBA Standalone Installation " topic in *UEBA Standalone Installation Guide*
Install NetWitness Server host.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Install 11.4 Log Hybrid Host.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Install and Configure NetWitness UEBA.	"Installation Tasks" topic in *UEBA Standalone Installation Guide*
Assign the UEBA_Analysts and Analysts roles to the UEBA users.	"Role Permissions" in the System Security and User Management Guide

Fresh Installation

The following tasks must be performed in the following sequence.

Description	References
	
Review the supported hardware.	"Supported Hardware" in the *Physical Host Installation Guide*
Review the UEBA architecture.	"NetWitness Platform Network Architecture Diagram" topic in the *Deployment Guide*
Configure the ports on your firewall.	"Network Architecture and Ports" topic in the *Deployment Guide*
Install NetWitness Server host and other components.	"Task 1 - Install 11.4 on the NetWitness Server (NW Server) Host" and "Task 2 - Install 11.4 on Other Component Hosts" in *Physical Host Installation Guide* "Install NetWitness Platform Virtual Host in Virtual Environment" in the *Virtual Host Installation Guide*
Install UEBA.	"RSA NetWitness® UEBA" in *Physical Host Installation Guide*
Assign the UEBA_Analysts and Analysts roles to the UEBA users.	"Role Permissions" in the *System Security and User Management Guide*

Update

The following tasks must be performed in the following sequence.

Description	References
	
Deploy the Endpoint Pack from RSA Live, which contains File Category Lua Parser for the UEBA integration with Endpoint.	During deployment, you must specify Endpoint Log Hybrid Log Decoder service. In case of multiple Endpoint servers, select all the Endpoint Log Hybrid Log Decoder services
Enable Endpoint data sources such as Process and Registry to generate alerts in UEBA.	"Enable Endpoint Data Sources" in the *Update Instructions*
Enable UEBA indicator forwarder to transfer the UEBA indicators to the NetWitness Respond server and to the correlation server to create an incidents.	"Enable UEBA Indicator Forwarder" in the *Update Instructions*

Description	References
After you update to NetWitness Platform 11.4 the Broker or Concentrator UUID changes. You must update the NetWitness Platform core services, and update the Broker or Concentrator UUID.	"Update Broker or Concentrator UUID" in the *Update Instructions*
Update Airflow Configuration.	"Update Airflow Configuration" in the *Update Instructions*
Restart the Airflow scheduler service after the presidio_ upgrade DAG is successful.	"Restart Airflow scheduler service" in the *Update Instructions*

Investigation

The following tasks can be performed in any sequence.

Description	References
	
Investigate high risk user and network entities.	"Investigate High-Risk Entities" topic in the *RSA NetWitness UEBA User Guide*
Investigate top alerts.	"Investigate Top Alerts" topic in the *RSA NetWitness UEBA User Guide*

Monitoring

The following tasks can be performed in any sequence.

Description	References
	
Review NetWitness UEBA metrics in Health and Wellness.	"View NetWitness UEBA Metrics in Health and Wellness" topic in the RSA NetWitness UEBA User Guide
Monitor Health and Wellness of UEBA.	"Monitor Health and Wellness of UEBA" topic in the RSA NetWitness UEBA User Guide